NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Barge sinks in Duluth harbor.** Workers are trying to recover a 1,000-gallon propane tank from a barge that sank in the Duluth harbor in Duluth, Minnesota, the Associated Press reported March 2. The U.S. Coast Guard (USCG) was working with salvage companies to get the nearly full tank off the sunken 120-foot-long barge, which sank in a harbor slip. The USCG said it does not know why the barge went down. The 106 year-old barge is owned by Duluth Timber Co. and will have to be removed if it is a navigation hazard or causes pollution. Source: http://www.news8000.com/news/Barge-sinks-in-Duluth-harbor/-/326/9199058/-/15aqmgkz/-/

National

Tornado wrecks Indiana town as Midwest is slammed with severe storms. Powerful storms stretching from the Gulf Coast to the Great Lakes flattened buildings in several states, wrecked a small Indiana town, and bred anxiety across a wide swath of the country, the Associated Press reported March 2. Widespread damage was reported in southern Indiana, where a Clark County Sheriff's Department official said the town of Marysville is "completely gone." Dozens of houses were also damaged in Alabama and Tennessee 2 days after storms killed 13 people in the Midwest and South. Thousands of schoolchildren in several states were sent home as a precaution, and several Kentucky universities were closed. The Huntsville, Alabama mayor said students in area schools sheltered in hallways as severe weather passed. At least 20 homes were badly damaged in the Chattanooga, Tennessee area after strong winds and hail lashed the area. In the Huntsville area, five people were taken to hospitals, and several houses were leveled by what authorities believed were tornadoes. An apparent tornado also damaged a state maximum security prison about 10 miles from Huntsville, but none of the facility's approximately 2,100 inmates escaped. An Alabama Department of Corrections spokesman said the roof was damaged on two large prison dormitories that each hold about 250 men. Part of the perimeter fence was knocked down, but the prison was secure. Source: http://www.foxnews.com/us/2012/03/02/alabama-schools-closing-early-amid-weather-threat/

Flooding costs top $1 billion. Costs revealed February 28 continue to push the bill for 2011 Missouri River flooding over $1 billion in the states of Nebraska, Iowa, Missouri, and Kansas. Early estimates indicate the U.S. Army Corps of Engineers' six big upriver dams prevented at least $7.6 billion in damage last year, said a spokesman who manages river programs for the Corps. He said the reservoir system provides an average $1.8 billion in annual benefits. The commander of the Omaha District said the $7.6 billion prevented-damage estimate is a "low-ball number" because it is based on 1970s-era information of which businesses, homes, crops, and developments exist in the river floodplain. However, the cost of flooding continues to climb, officials said. Nearly 1,100 Nebraskans and 1,300 Iowans have sought individual assistance from the Federal Emergency Management Agency. Officials said the cost of repairs to dams and levees will climb as engineers continue inspections and find soft spots in levees, for example. Seepage is a primary concern in 2012 because floodwater was on the levees for a long time and could have created a capillary effect through the earthen structures. Repairs to five holes in levees protecting the Hamburg, Iowa, and Rockport, Missouri, areas now are substantially complete, officials reported. Crews worked through the night February 27 to finish closing the third and final breach in the Hamburg area before a rainstorm February 28. The levees have been rebuilt to original height and width. Officials said the five projects represented the most critical repairs in the levee system damaged during 2011's flood. Source: http://www.omaha.com/article/20120228/NEWS01/702289888

'Devastation ... like we've never seen' in twister-hit town. At least 9 people were killed February 28-29 as a line of tornadoes marched across the Midwest. Forecasters warned more twisters could strike the Tennessee Valley and southern Appalachians through February 29. Six of the deaths and nearly 100 injuries occurred in Harrisburg, Illinois, after an EF-4 tornado swept through, destroying at least 200 homes and more than 25 businesses. Three other deaths were reported in Missouri, where storms included a suspected tornado that hit a mobile home park outside the town of Buffalo. One person died in the mobile home park and around a dozen people were injured. Two others died in the Cassville and Puxico areas of Missouri. In Harrisburg, police issued a curfew overnight and the area most impacted was evacuated as a precaution. Some 3,300 customers were without power in the town of about 10,000. About 12 people were injured when an EF-2 tornado ripped through Harveyville, Kansas. At least three of the injured are in critical condition, according to Weather.com, and 40 percent of the town suffered damage. KSHB 41 Kansas City reported an apartment complex and a church were among the damaged buildings A tornado with a preliminary rating of EF-2 moved through Branson, Missouri, injuring 32 people and heavily damaging the city's famous theaters and moving up Highway 76, uprooting road signs and scattering debris. The assistant general manager for the 530-room Hilton and adjacent Branson Convention Center, noted windows were shattered and some rooms had furniture sucked away by high winds. Hotel workers were able to get all guests to safety as the storm raged. The owner of the damaged Cakes-n-Creams '50s Diner said the theater next to his business "kind of exploded", and the hotels "on the two sides of me lost their roofs." Newburgh, Indiana, and Kingsport, Tennessee, also reported storm damage. Source: http://usnews.msnbc.msn.com/_news/2012/02/29/10536654-4-killed-as-tornadoes-rake-midwest-states

International

Nothing Significant to Report

Banking and Finance Industry

Bogus US SEC notification leads to malware. Notifications purportedly sent by the U.S. Securities and Exchange Commission have been hitting in-boxes and trying to trick users into following a malicious link, GFI warned March 2. Those who open the link included in the e-mail will be redirected through a number of sites and will finally end at one that hosts the Blackhole exploit kit, which is able to take advantage of many Adobe Reader, Acrobat and Flash vulnerabilities, as well as some in Java and Windows Media Player. If the kit manages to exploit one of those, the user is taken to a Web site where he can download the about.exe file. This is not a document containing details of the complaint, but a variant of the Zeus/Zbot information-stealing trojan that is currently detected only by a dozen of the AV solutions employed by VirusTotal. Source: http://www.net-security.org/malware_news.php?id=2022

Americans lost $1.52 bln to identity theft, scams in 2011. Identity theft and other scams cost Americans $1.52 billion in 2011, the Federal Trade Commission (FTC) said February 28. In a nationwide sampling of consumer complaints, law enforcement, and other agencies received 1.8 million complaints in 2011, up from 1.4 million in 2010 and double the level in 2006, the FTC said in a statement. Identity theft remained the top category. The increase reflects the growing number of agencies that contributed to the Consumer Sentinel Network, a database that is the basis of the report, rather than an upturn in fraud, the head of the FTC's planning and communications unit told Reuters. Identity theft "has been our No. 1 complaint generator for the past 5 years, and that seems to be consistent" at 15 percent of complaints in 2011, he said. Fraudsters increasingly are using the Internet and e-mail to carry out scams or identity theft rather than by telephone or mail, he said. Source: http://www.chicagotribune.com/sns-rt-usa-consumerfraudl2e8dsbi3-20120228,0,2334070.story

FBI fraud probes increase as insider trading 'widespread'. Open FBI investigations into corporate, securities and commodity fraud increased 8.8 percent as of September 30, 2011, compared to 2010, the agency said in a report released February 27. The FBI had 2,572 such cases open at the end of the 2011 fiscal year, according to the report, up from 2,364 in 2010. The FBI report included data on financial crime probes during 2010 and 2011. There was an increase in insider trading probes, which are a "widespread problem" that has plagued the "fair and orderly operation" of securities markets, the report noted. The FBI is making greater use of wiretaps and undercover operations, which may provide the "best evidence" to prosecute financial crimes, the chief of the FBI's financial crimes section said at a briefing in Washington, D.C. The FBI used wiretaps or undercover operations in more than 40 corporate, securities, and commodity cases in 2011, compared to less than 20 in 2008. The number of cases involving falsified financial data "remains relatively stable," according to the report. The number of pending mortgage fraud cases declined 14 percent to 2,691 in 2011 from the 2010 fiscal year. Fraud targeting distressed homeowners has displaced loan originations as the biggest source of fraud in many FBI field offices, the report said. The FBI also had 2,690 pending health care fraud investigations at the end of fiscal 2011, up from 2,573 in 2010. Source: http://www.businessweek.com/news/2012-02-27/fbi-fraud-probes-increase-as-insider-trading-widespread-.html

Russian man pleads guilty to cyber-fraud conspiracy in U.S. A Russian national charged by U.S. authorities with orchestrating a cyber-fraud scheme from Europe has pleaded guilty to illegally gaining computer access to bank accounts via Web sites claiming to offer goods and merchandise, Bloomberg reported February 24. He pleaded guilty in federal court in Manhattan

February 17 to a count of conspiracy and a count of wire fraud, records show. Federal prosecutors alleged a scheme from 2004 to 2005 involving the man, his son, and others preying on U.S. consumers who believed the unauthorized charges were for legitimate goods. They said the father, son, and unidentified accomplices controlled U.S.-registered companies Sofeco LLC, Pintado LLC, and Tallit LL that appeared to be legitimate Internet merchants. The defendants took unauthorized charges on customers' credit cards, prosecutors said. They also got credit card numbers by buying them from people or by using computer programs surreptitiously installed on victims' computers. The pair engaged in a scheme from June 2004 to February 2005 to access financial services accounts of U.S. victims and attempted to transfer hundreds of thousands of dollars into bank accounts they controlled, prosecutors said. The defendants also bought and sold securities in publicly traded companies through a firm called Rim Investment Management Ltd. Source: http://www.businessweek.com/news/2012-02-24/russian-man-pleads-guilty-to-cyber-fraud-conspiracy-in-u-s-.html

Chemical and Hazardous Materials Sector

US NRC to propose first post-Fukushima safety rules. U.S. nuclear regulators moved to issue new rules to deal with safety issues raised by the Fukushima nuclear accident, Reuters reported March 1. Three members of the Nuclear Regulatory Commission (NRC) voted to issue the first of three proposed rules recommended by the agency staff, although the commissioners differed on some details. The staff said its recommendations, based on eight changes identified by the NRC's Fukushima task force, could move forward without significant delay, with implementation by the end of 2016. Source: http://www.reuters.com/article/2012/03/01/utilities-nrc-fukushima-idUSL2E8E1GTQ20120301

Commercial Facilities

Nothing Significant to Report

Communications Sector

(Virginia) **Pentagon suffers Internet access outage.** An unspecified number of U.S. Defense Department personnel in the Washington D.C. area and in the Midwest were cut off from the public Internet for nearly 3 hours March 1 because of technical problems, a department spokeswoman said March 2. The outage was not caused by any malicious activity, said the spokeswoman, who is an Air Force lieutenant colonel. She said the networks were back up and operating at normal capacity. The department's Defense Information Security Agency worked with commercial vendors and "mission partners" to reroute critical DoD traffic and to mitigate the issue until technical issues were resolved, she said. The number of people affected by the outage was not known, "but is estimated in the thousands, given the number of people who work in the Pentagon," the lieutenant colonel told Reuters. Source: http://www.reuters.com/article/2012/03/02/us-cyber-pentagon-idUSTRE8211F220120302

Microsoft's Azure cloud suffers serious outage. Microsoft's Azure cloud infrastructure and development service experienced a serious outage February 29, with the system's service management component going down worldwide. "We are experiencing an issue with Windows Azure ... Customers will not be able to carry out service management operations," Microsoft said in an initial message on the outage on its Azure service dashboard. The issue has been "mitigated and service management is restored for the majority of customers," Microsoft said in a message. The incident's root cause was traced back to a cert issue. Microsoft said less than 3.8 percent of hosted services had been affected, and measures had been taken to stop the problem "from spreading across the production environment." In addition, Azure customers in the north and south central United States as well as northern Europe may experience performance problems, according to a message on the dashboard. "Deployed applications will continue to run. There is no impact to storage accounts either," it stated. The SQL Azure Data Sync service was unavailable in six regions around the United States., Europe, and Asia, and various problems were listed for some regions regarding Access Control 2.0, Azure Reporting, Azure Marketplace, and Azure Service Bus. The notifications promised regular updates on the work being done to fix the issues, but no concrete timetables. Source: http://www.pcworld.com/businesscenter/article/251043/microsofts_azure_cloud_suffers_serious_outage.html

FTC action leads to court orders banning marketers from selling vacation packages. The operators behind a vacation prize scheme have been banned from selling vacation packages under settlements with the U.S. Federal Trade Commission (FTC) and the Florida Attorney's General Office, which charged the defendants with tricking consumers into believing they had won a vacation package as a prize, and then failing to provide the package as promised, according to a February 28 release. According to the complaint, the defendants advertised a vacation package worth thousands of dollars as a prize to consumers who called a toll-free number and answered a trivia question. Callers were told they had won, and that if they paid up to $400 in "taxes" or "fees" they would receive their prize. The complaint alleged callers did not receive the vacation packages as promised. The defendants are VGC Corporation of America, also doing business as All Dream(s) Vacations, All Dreams Travel, Five Star(s) Vacations, 5 Star(s) Vacations, Total Tours, and Travel & Tours Corp.; All Dream Vacations Corp., also doing business as All Dreams Vacations; and three individuals. The orders also impose a judgment of more than $14 million, which will be suspended on the satisfaction of numerous terms and conditions designed to ensure that the defendants will be stripped of all of their assets of value. Source: http://www.ftc.gov/opa/2012/02/vgc.shtm

Critical Manufacturing

NHTSA recall notice - Volvo S60, S80, XC60, XC70 seat wire harnesses. Volvo announced March 2 the recall of 17,000 model year 2012 S60, S80, XC60, and XC70 vehicles manufactured from May 16, 2011 through October 6, 2011. The wire harness under the front seats may have not been attached properly to the seat frame. As a result, when the seats are moved to adjust the seating position, the wire harness may get pulled, causing it to disconnect. In the event of a crash, the front and/or side impact air bags may deploy improperly or not at all, increasing the risk of injury. Also, the lap belt pretensioner may not deploy. Volvo will notify owners, and dealers will inspect and, if necessary, secure the seat wire harness. The safety recall is expected to begin March 30. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V075000&summary=true&prod_id=1181768&PrintVersion=YES

American Honda recalls trimmers due to laceration hazard. The U.S. Consumer Product Safety Commission and Health Canada, in cooperation with American Honda Motor Company announced a voluntary recall of about 17,600 Honda Grass Trimmers February 28. Consumers should stop using recalled products immediately unless otherwise instructed. The shaft can crack and cause the lower gear case and cutting attachment to detach, posing a laceration hazard to the operator and bystanders. Honda is aware of 11 incidents of broken or cracked shafts. No injuries were reported. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12121.html

NHTSA recall notice - Infiniti M and QX, and Nissan Juke fuel pressure sensors. Nissan announced February 27 the recall of 79,275 model year 2011-2012 Nissan Juke, Infiniti QX, and Infiniti M vehicles. The fuel pressure sensor may loosen due to heat and vibration causing fuel to leak. Fuel may leak from the pressure sensor, increasing the risk of a fire. Nissan will notify owners, and dealers will replace the fuel pressure sensors as necessary. The safety recall is expected to begin March 19. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V069000&summary=true&prod_id=877868&PrintVersion=YES

Defense/ Industry Base Sector

(California) **Planned missile test postponed.** A Minuteman 3 test planned for March 1 from Vandenberg Air Force Base in California was postponed so crews could swap out a possibly problematic part, officials said. “The test launch is delayed in order to replace a test-unique tracking component used only on test missiles,” Air Force Global Strike Command officials said. “The test-unique tracking component monitors missile location within geographic boundaries of the test range.” A new launch date has not been set yet, officials said. The test was scheduled to occur between 2:01 a.m. and 8:01 a.m. from an underground silo. However, February 27, officials at Air Force Global Strike Command decided to delay the launch, citing a review of data from a Minuteman 3 test February 25. That unarmed Minuteman missile launched successfully at 2:46 a.m., Global Strike Command officials said of the mission dubbed Glory Trip-203. “Based on system performance analysis during GT-203 and an assessment of like components in the inventory, engineers have determined there is a potential for loss of signal continuity in one of the redundant tracking systems,” they said. “We do not know for sure if there is a problem with the test missile originally scheduled to launch ...; however, engineers have recommended that the component in question be replaced.” Replacing the part should take 3 to 4 days, officials added. Source: http://www.lompocrecord.com/news/local/military/vandenberg/planned-missile-test-postponed/article_13492e9a-6367-11e1-a651-0019bb2963f4.html

Man charged in plot to export military technology. An Australian man and his company were charged February 29 in a scheme to export to Iran components for drones, torpedoes, missiles, and other military technology. A five-count indictment returned in Washington, D.C., accuses the man of knowingly skirting a federal trade embargo with Iran and plotting to export the technology without the required authorization. Prosecutors said the man and his company, ICM Components, Inc., ordered aircraft parts and other goods from U.S. companies on behalf of a representative of an Iranian trade company. The man concealed the fact the goods were intended for shipment to Iran, sometimes placing orders through a Florida-based broker, and duped manufacturers, shippers, and distributors about their intended end-use, the indictment alleges. The man, identified by prosecutors as the general manager of ICM, remains at large and is believed to be living in Australia. The company is also named in the indictment. The company representative who worked with the man, identified in court papers only as "Iranian A," would not have been able to directly purchase the goods from the United States on his own, prosecutors said. The alleged export scheme spanned about 2 years starting around March 2007. The indictment charges the ICM general manager with four separate exports or attempted exports, including two separate shipments of mounted light assemblies for use on helicopters and fixed-wing aircraft; a shipment of precision pressure inducers that can measure altitude and record barometric pressure; and a shipment of emergency flotation kits, which can help a helicopter landing in water or on soft desert terrain. The indictment charges the man and the company with conspiracy, and with four counts of illegally exporting goods to an embargoed nation. Source: http://www.times-standard.com/ci_20071950

Emergency Services

(Texas) **Texas 'navy' to patrol the Rio Grande.** In March, the Texas Department of Public Safety will deploy the first of a fleet of six gunboats on the Rio Grande, the river that forms the border between Texas and Mexico, WFAA 8 Dallas reported February 29. The 34-foot-long boats, each powered by 3,300-horsepower outboard engines, will have bulletproof plating and 6 machine guns apiece. The vessels will be able to operate in as little as 2 feet of water, according to the report, and will work with U.S. Customs and Border Protection to combat drug smuggling coming across the Rio Grande. Source: http://news.blogs.cnn.com/2012/02/29/texas-navy-to-patrol-the-rio-grande/?hpt=us_c2

(Florida) **'SWATing' hoax triggers emergency response.** Sheriff's investigators are trying to track down who made a hoax call to emergency operators in Sarasota, Florida, over the weekend of February 25. The caller who identified himself as a 15-year-old, claimed he shot his parents and was armed with a gun. He also claimed to have a bomb strapped to himself, set to detonate within 10 to 15 minutes. "Ultimately there were almost three dozen law enforcement officers dispatched, hostage negotiators, SWAT team, and every available deputy," said a Sarasota County Sheriff's Office spokeswoman. But when deputies arrived, they found an unsuspecting family, no one shot, and no guns. In fact, investigators said the call did not even come from the home. It is part of a troubling trend called "SWATing." The prankster obtains information about their intended target then call in posing as that person with a story that triggers a SWAT-style response. If caught, the prankster could potentially face federal charges punishable by decades behind bars. Source: http://www.wtsp.com/news/article/241436/8/SWATing-hoax-triggers-emergency-response-

(Ohio) **NORIS computer system shut down over virus.** A critical computer network was down for a third day, February 24, after falling victim to a sophisticated worm. The failure impacted about 200 different agencies, including police departments, jails, and courts in northwest Ohio. A computer worm infected the Northwest Ohio Regional Information System (NORIS) causing the shutdown February 22. It is unclear what caused the problem, but system administrators believe it was unlikely from hacking. The Toledo Police Department (TPD) uses the system to check for warrants, criminal histories, mug shots, and other records on laptops while patrolling. "We're unable to run records, checks license plates and other things of that nature through NORIS. We have other means of doing it, but this clearly is slowing us down," said an Oregon Police Department sergeant. Source: http://www.wtol.com/story/17011513/noris-computer-system-shut-down-over-virus

Energy

GAO: Improved public-private collaboration required to ensure cybersecurity of electric grid. The federal government can improve the cybersecurity of the electric grid by coordinating oversight of industry compliance with voluntary security standards, implementing an effective information-sharing system with the electric industry, and encouraging companies to build security into "smart" grid devices, a new government report found. Government Accountability Office (GAO) investigators presented the results of their study to a House panel February 28. They also presented previous recommendations that the Federal Energy Regulatory Commission (FERC) should improve its coordination with other government regulators in the monitoring of cybersecurity compliance by electric companies. Without sharing and coordinating their observations, federal agencies have no way of knowing if voluntary standards are effective, experts warned in their report, "Cybersecurity: Challenges in Securing the Modernized Electricity Grid." The FERC, the primary oversight agency for the electric industry, also lacks an effective information-sharing mechanism to communicate with companies, said the GAO director of information security, and GAO director of natural resources and environment, before a House Energy and Commerce subcommittee. The electric industry has an information-sharing center, but it has not used it to address the sharing of cybersecurity information. Source: http://www.hstoday.us/briefings/daily-news-briefings/single-article/gao-improved-public-private-collaboration-required-to-ensure-cybersecurity-of-electric-grid/284b68512ed3b1582194c162fa800af4.html

U.S. report: Fuel markets 'significantly impacted' by refinery shutdowns. The U.S. Department of Energy February 27 said fuel markets in the Northeast "could be significantly impacted" if Sunoco closes its Philadelphia refinery in June, leading to tight supplies and price spikes in some areas. The report from the U.S. Energy Information Administration (EIA) said supplies of ultra-low sulfur diesel would be most affected by refinery shutdowns and transportation constraints. The potential loss of the Sunoco Philadelphia refinery "presents a complex supply challenge, and no single solution has been identified by industry participants that will address all of the logistical hurdles that must be overcome." Pittsburgh and western New York state, which now are supplied through pipelines from the Philadelphia refineries, would most likely suffer if supplies of diesel and heating oil were constrained. Sunoco, headquartered in Philadelphia, announced in 2011 it would shut down its 335,000 barrel-per-day refinery if it could not find a buyer by June. The plant along the Schuylkill accounts for 24 percent of the refining capacity in the Northeast. Source: http://www.philly.com/philly/news/homepage/140663913.html

Food and Agriculture

Campylobacter cases from raw milk outbreak reach 80. The Pennsylvania Department of Health confirmed more cases of Campylobacter infections in an outbreak tied to contaminated unpasteurized milk from Your Family Cow dairy in Chambersburg, Pennsylvania. The latest cases bring the outbreak toll to 80 confirmed illnesses, Food Safety News reported March 1. This is the largest foodborne illness linked to raw milk in Pennsylvania history, affecting individuals in four states. The breakdown of cases by state is as follows: Pennsylvania (70 illnesses), Maryland (5), West Virginia (3), and New Jersey (2). Since 2007, Pennsylvania raw milk dairies have been linked to at least 7 outbreaks, now resulting in a total of 287 illnesses. llness onset dates for the current outbreak range from January 17 to February 1. At least nine people have been hospitalized. Although the Your Family Cow dairy temporarily halted sales upon discovery of the outbreak, the farm was allowed to resume production February 6, after passing a health inspection. Source: http://www.foodsafetynews.com/2012/03/campylobacter-cases-from-pa-raw-milk-outbreak-reach-80/

Outbreak linked to raw sprouts grows to 14 cases, six states. Two new cases, both from Michigan, were confirmed in the multistate outbreak of E. coli O26 linked to raw clover sprouts served at Jimmy John's restaurants in six states, the Centers for Disease Control and Prevention (CDC) reported February 24. That brings the outbreak total to 14. Both new cases said they ate sprouts at Jimmy John's restaurants in the week before they became ill. Iowa has reported five cases tied to the outbreak, Missouri has reported three, while Kansas and Michigan each have reported two cases. Arkansas and Wisconsin each have reported one outbreak-connected case. In its initial report, the CDC said the traceback probe had implicated a common lot of clover seeds used at two separate sprouting facilities. Both growers supplied sprouts to Jimmy John's restaurants. Raw sprouts served at Jimmy John's restaurants have been tied to 5 outbreaks in 4 years. Source: http://www.foodsafetynews.com/2012/02/outbreak-linked-to-raw-sprouts-grows-to-14-cases/

Government Sector (including Schools and Universities)

As deadline nears, federal agencies mostly free of DNSChanger. Although millions of computers around the world could still contain the DNSChanger malware used by an Internet fraud ring, government agencies and large enterprises appear to have done a good job of cleaning up the infections, said a member of the DNSChanger Working Group, Government Computer News reported March 1. The member said early in February that, based on information gleaned from traffic to rogue DNS servers, it appeared that half of all Fortune 500 companies and 27 of 55 major federal agencies were infected. He reported at the RSA Conference that, as of February 23, those numbers had dropped to just 3 agencies and 94 companies. The progress is important, because the non-profit Internet Systems Consortium has been operating the name servers under a court order on behalf of the Justice Department since November 2011 to ensure infected computers whose DNS requests were being directed to the rogue servers were not cut off from the Internet. The original court order expires March 8. However, there still are a large number of computers that must be cleaned up, and it is not known how many computers are infected within each agency or company. “It’s hard to know exactly how many machines,” he said. “It’s probably millions.” However, from traffic volumes, the number appears small at government agencies. Source: http://gcn.com/articles/2012/03/01/rsa-13-federal-dnschanger-cleanup.aspx

(Arizona) **Student hurt, man jailed in Ariz. school shooting.** Authorities worked to determine what motivated a man to allegedly fire a rifle indiscriminately at a Willcox, Arizona high school, injuring a student who was watching a baseball game. The student suffered minor cuts from flying glass when the car he was in was shot at March 1, authorities said. The man was arrested shortly after the shooting at Willcox High School, and the weapon he was accused of using was recovered about a block from the scene, according to the Willcox Department of Public Safety (DPS). The DPS chief said authorities believe he fired three rounds. Source: http://www.chron.com/news/article/Student-hurt-man-jailed-in-Ariz-school-shooting-3375159.php

NASA: Hackers targeted us 5,408 times in 2010 and 2011. Written testimony the Inspector General (IG) at NASA submitted to a Congressional committee said the agency suffered more than 5,000 security incidents in 2010 and 2011, Softpedia reported March 1. They “spanned a wide continuum from individuals testing their skill to break into NASA systems, to well-organized criminal enterprises hacking for profit, to intrusions that may have been sponsored by foreign intelligence services seeking to further their countries’ objectives,” the IG wrote. The intrusions apparently damaged thousands of computing devices, with the total estimated cost to NASA being more than $7 million. The IG admitted the organization is far behind other agencies when it comes to protecting the laptops utilized by personnel. In the time frame between April 2009 and April 2011, 48 laptops and other mobile devices were stolen. As a result of these incidents, not only was personally identifiable information leaked, but also more important data, such as algorithms used to control the International Space Station, and secret data on NASA’s Constellation and Orion projects. The biggest issue is not that the devices were stolen, instead the problem is that most of them had no form of encryption implemented. Advanced persistent attacks also targeted NASA. In the fiscal year 2011, 47 such attacks were reported, 13 of which were successful. Source: http://news.softpedia.com/news/NASA-Hackers-Targeted-Us-5-408-Times-in-2010-and-2011-255951.shtml

Springfield city Web site hacked. A Springfield, Missouri official said the personal information of about 2,100 people may have been obtained by hackers when the city's Web site was "compromised" February 17. Some functions were turned off on the city's Web site, as authorities investigate the apparent breach, said the city spokeswoman. She said officials are notifying the 2,100 individuals who may have been victimized. She said those who were at risk will receive a letter offering a 1-year subscription with an identity theft protection company. The spokeswoman said the Web site last passed a security scan February 8. She said the city is reviewing security measures and making modifications to prevent future incidents. Source: http://www.news-leader.com/article/20120227/NEWS01/302270075/

Information Technology and Telecommunications

Anonymous Web weapon backfires with hidden banking Trojan. Anonymous supporters queuing up to participate in denial-of-service attacks are being tricked into installing ZeuS botnet clients. Hacktivists grabbed what they thought was the Slowloris tool, which is designed to flood Web sites with open connections and ultimately knock them offline. However, the download included a strain of ZeuS, which promptly installed itself on their Microsoft Windows machines. The trojan will carry out the distributed attacks, but that's not all it does — it will also steal users' online banking credentials, Web mail logins, and cookies. The deception began January 20, Symantec reported. Malware peddlers swiped the template of an Anonymous guide to launching denial-of-service attacks from Pastebin, modified it to include a link to Slowloris, and reposted the message on Pastebin to snare victims. Source: http://www.theregister.co.uk/2012/03/02/trojan_attack_tool_targets_hacktivists/

Multiple vulnerabilities found in Pinterest. Pinterest, a pinboard social media Web site, was found to contain many vulnerabilities that could allow an attacker to cause serious damage. A security researcher found the site, which has more than 10 million active users, has extremely poor security. He identified a cross-site scripting vulnerability and an iframe injection issue that could allow hackers to hijack user accounts and perform other malicious operations. With the aid of another security researcher, he found a URL redirection flaw that could be leveraged to redirect the site's visitors to other potentially malicious domains. Source: http://news.softpedia.com/news/Multiple-Vulnerabilities-Found-in-Pinterest-Exclusive-255797.shtml

Malware increasingly uses DNS to avoid detection, experts say. The number of malware threats that receive instructions from attackers through domain name system (DNS) is expected to increase, and most companies are not currently scanning for such activity on their networks, security experts said February 28 at the RSA Conference 2012. There are many channels attackers use for communicating with their botnets, ranging from traditional ones such as TCP, IRC, and HTTP to more unusual ones such as Twitter feeds, Facebook walls, and even YouTube comments. Most malware-generated traffic that passes through these channels can be detected and blocked at the network level by firewalls or intrusion prevention systems. However, that is not the case for DNS and attackers are taking advantage of it, said the founder of Counter Hack Challenges and SANS fellow during a presentation on new attack techniques.

The DNS protocol is normally used for a precise critical function — the translation of host names into IP addresses and vice-versa. Because of this, DNS traffic does not get filtered or inspected by traffic monitoring solutions and is allowed to flow freely through most networks. As DNS queries gets passed from one DNS server to another until they reach the authoritative servers for the respective domains, network-level IP blocklists are useless at blocking them. Source: http://www.computerworld.com/s/article/9224743/Malware_increasingly_uses_DNS_to_avoid_detection_experts_say?taxonomyId=17

UN.org, Skype.com, and Oracle.com hacked by D35m0nd142. Grey hat hacker D35m0nd142 managed to gain unauthorized access to the sites of the United Nations, Skype, and Oracle. On the official Skype site, the hacker found Blind SQL injection vulnerabilities that allowed him to access their Web server. A similar vulnerability was discovered on Oracle's community site, which can allow hackers to cause serious damage. By leveraging an MSSQL injection flaw, he managed to bypass the security protocols implemented by the United Nations site administrators. In each scenario, the hacker ensured the data he accessed remained unharmed and contacted the ones responsible for the sites to notify them of the presence of the issues. Source: http://news.softpedia.com/news/UN-org-Skype-com-and-Oracle-com-Hacked-by-D35m0nd142-255812.shtml

U.S. firm posts PLC hacking methods online. A U.S. information security company posted hacking techniques for disabling programmable logic controllers (PLCs) on the Internet, the Yomiuri Shimbun learned. A PLC is an electronic control system that enables machinery to work as programmed and is widely used in production systems at factories and in critical infrastructure. Alarmed by the hacking method released online by U.S. firm Digital Bond, Inc., DHS's Industrial Control Systems Cyber Emergency Response Team issued a warning stating cyberattacks against PLCs could cause a major systemic breakdown. Four companies in the United States, Japan, and France produce PLC control systems for automakers, electric power substations, and others. Digital Bond stated it posted the hacking method to "inform the public of the risks" of PLC breakdowns, arguing companies and governments have been slow to cope with PLCs' vulnerabilities. About 2 million PLC units per year are manufactured in Japan, approximately 1.4 million of which were exported. While cyberattacks targeting computer control systems have sharply increased overseas, this is the first time a Japanese PLC maker was revealed to be exposed to the risk of a cyberattack. The firms put at risk by Digital Bond's post are: Japan's Koyo Electronics Industries Co.; the United States' General Electric Co. and Rockwell Automation, Inc.; and France's Schneider Electric SA. After figuring out the design flaws of the companies' PLCs, Digital Bond posted programs attacking them on the firms' Web sites February 14, according to the U.S. network security company. Koyo Electronics said it sells several thousands of its PLCs domestically, as well as in the United States and other countries every year. The control systems are mainly used at automobile, semiconductor, and machine tool plants. Should the disclosed hacking techniques be abused, there is a danger the systems involved could be illegally controlled by a remote party. The PLCs made by the remaining three manufacturers feature designs that are different from each other, and are also used at a wide range of factories and transformer stations. Should these systems be hacked using Digital

Bond's methods or other tricks, production and other systems would break down or develop anomalies such as abnormal restarts. However, no direct links to Digital Bond's post have been confirmed, industry sources said. Source: http://www.yomiuri.co.jp/dy/national/T120228005028.htm

Malware authors expand use of domain generation algorithms. Malware authors are increasingly adopting flexible domain generation algorithms (DGAs) to evade detection and prevent their botnets from being shut down by security researchers or law enforcement agencies. DGAs are generally used as a fallback mechanism for sending instructions to infected computers when the hard-coded command and control servers become unavailable. The algorithms generate a list of unique pseudo-random domain names every day. Clients ina botnet attempt to connect to them and receive commands when the primary servers cannot be reached. Knowing the algorithm allows malware authors to predict which domain names infected computers will attempt to access on a certain date, so they can register one of them in advance. Source: http://www.computerworld.com/s/article/9224700/Malware_authors_expand_use_of_domain_generation_algorithms?taxonomyId=17

Anti-phishing DMARC adoption gathers (free) steam. The world's biggest names in the consumer Web mail space are sharing security intelligence with businesses for free to help drive adoption of the Domain-based Message Authentication, Reporting, and Conformance (DMARC) e-mail authentication system. In January, Google, Microsoft, AOL, Facebook, and Yahoo! joined up with service providers such as PayPal to push the DMARC standard, which integrates with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) systems. The advantage of participating in DMARC for businesses is that they, as domain name holders, can specify e-mail handling policy via DMARC, which acts as an overlay for SPF and DKIM checking. By confirming an e-mail message is actually coming from a firm's servers and not from a spammer, spoofed e-mails are cut out, and info about that spam-blocking is then fed back into the DMARC register to identify the e-mail systems being used by the spammers. The open flow of information between DMARC and businesses ensures both sides benefit from more efficient spam blocking. The week of February 20, the e-mail intelligence firm and founding member of the DMARC consortium Agari opened up its Receiver Program, making it free to all comers. Businesses can sign up to get the latest anti-spam and anti-phishing intelligence from members of DMARC, and can use it to refine filtering techniques. Source: http://www.theregister.co.uk/2012/02/24/dmarc_spam_phishing_free/

Cyber intrusions into Air Force computers take weeks to detect. When a hacker manages to penetrate U.S. Air Force computer networks, it generally takes experts more than a month to piece together what went wrong, the National Defense Industrial Association reported February 24. A forensics investigation into a network breach lasts an average of 45 days, said the senior adviser for intelligence and cyber-operations for the 24th Air Force, the organization that operates and defends the service's networks. "That's way better than we used to be, but that's not tactically acceptable," he told an Armed Forces Communications and Electronics Association (AFCEA) information technology conference. The Air Force needs hardware and software that leaves no back doors to the network open, officials said. Currently, if hackers find a hole they can unload “truckloads of information” without the service even knowing they were even on the network, said the inspector general of the Air Force. Officials asked for industry help to improve its ability to watch over the network and detect and respond to unauthorized activity. Source: http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=688

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

McAfee hacker says Medtronic insulin pumps vulnerable to attack. Some Medtronic Inc. insulin pumps are vulnerable to a hacking attack that could let someone break into the devices from hundreds of feet away, disable security alarms, and dump insulin directly into diabetics’ bloodstreams, according to a computer-security researcher at McAfee Inc. The McAfee researcher said he can remotely control several types of Medtronic pumps. After first discussing the vulnerability last year at a small hacker conference in Florida, he has discovered more ways to exploit the weakness, including overriding security features such as vibration warnings. He is trying to increase awareness of the risks of medical devices. Medtronic has responded to the risks by hiring security teams from three organizations to inspect its products. Medical-device security first became a flash point last year when a diabetic patient in Idaho showed hackers could manipulate the best-selling brand of pump he used. He got the attention of lawmakers, who pressed the Government Accountability Office to investigate whether the industry’s cybersecurity rules are tough enough. The report from that probe is due in July. Source: http://www.bloomberg.com/news/2012-02-29/mcafee-hacker-says-medtronic-insulin-pumps-vulnerable-to-attack.html

Sleeping pills linked to almost fourfold increase in death risk. Adults who take sleeping pills in even small numbers over their lifetimes may be nearly four times more likely to die earlier compared to those who are not prescribed sleeping pills, according to new findings published February 27 in the British Medical Journal. And those prescribed sleeping pills may also be more likely to be diagnosed with cancer, the study found. Researchers looked at electronic medical records of nearly 35,000 patients, fewer than half of whom took such U.S. Food and Drug Administration-approved sleep medications as Ambien, Restoril, Lunesta, and Sonata. They found that even those who look fewer than 18 sleeping pills a year were at greater risk of death, compared to those who were not prescribed sleeping aids. Source: http://abcnews.go.com/Health/Sleep/sleeping-pills-linked-times-increased-death-risk/story?id=15803687#.T0zgC4Hy3cs

Transportation

(Colorado) **No explosives found on United plane after bomb threat.** Authorities said no explosives were found after a bomb threat was reported involving a United Airlines plane at Denver International Airport in Denver. The FBI said the bomb threat was called in March 1, but officials said they did not know who took the call. Because the threat had specific information about the flight, officials took the threat very seriously. The Transportation Safety Administration (TSA) initially said passengers were evacuated and the plane was moved from Concourse B to an area next to an airport fire station. However, TSA then corrected that statement, saying passengers were never on the plane, but they were moved to another area away from the concourse. It is not clear if the passengers and their carry-on luggage were re-screened. There the plane was searched, but no explosives were found. TSA officials said the passengers were put on another airplane for the flight to San Francisco. Source: http://www.thedenverchannel.com/news/30578201/detail.html

Water and Dams

(New Jersey) **EPA approves New Jersey's list of polluted water bodies; Sewage pollution continues to be a major problem in New Jersey.** The U.S. Environmental Protection Agency (EPA) approved the 2010 list of waters in New Jersey that are considered impaired or threatened by pollutants February 28. The list helps establish priorities for addressing threats from water pollution. The Clean Water Act (CWA) requires states to assess water quality and to report findings every 2 years. Compiled by the New Jersey Department of Environmental Protection, the list is a tool for reaching the goal of "fishable and swimmable" waters. The list specifically includes impaired waters for which the development of budgets for the amount of water pollution allowed is necessary. The budgets define the maximum amount of a pollutant a water body can receive and still meet water quality standards. They are developed by states and approved by the EPA once the agency determines the budget will allow the body to achieve water quality standards. The most common pollutants causing impairment in New Jersey water bodies include PCBs (8.33 percent), dissolved oxygen (8.19 percent), phosphorus (7.86 percent), pH (7.62 percent), and arsenic (6.89 percent). The list also notes the most common sources of water pollutants, which include urban/stormwater runoff, combined sewer overflows from systems that capture domestic sewage and stormwater, and air pollution, including acid rain. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/0B9E3346E99EDDC5852579B2005408D3

(Indiana) **Leaky pipes cost city 15% of treated water.** Aging water pipes leak millions of gallons of water into the ground through breaks or tiny cracks, costing Fort Wayne, Indiana, more than a half-million dollars in 2011, the Fort Wayne Journal Gazette reported February 25. Of the 10.7 billion gallons of water produced at the city utilities plant in 2011, 23 percent was never sold to a customer. Some of this unsold water is used to flush fire hydrants or water lines, fight fires, or clean sewers. But the vast majority, city officials estimate it is 15 percent of total water produced, is simply lost to the ground. This means the city produced 1.6 billion gallons of water last year that served no purpose other than to make area soils a little wetter. It costs the city about $550,000 to produce that lost water, according to a utility spokeswoman, costs eventually passed on to utility customers. The amount of water not billed, not simply lost, grew from 1.8 billion gallons in 2007 to nearly 2.5 billion gallons in 2011. While the numbers might seem high, they are within industry norms, according to the utility's deputy director of engineering. Source: http://www.journalgazette.net/article/20120225/LOCAL/302259978

Water infrastructure bill to top $1 trillion: AWWA 'Buried No Longer' report highlights cost of repair, expansion; shows impact on U.S. households. The cost of repairing and expanding U.S. drinking water infrastructure will top $1 trillion in the next 25 years, an expense that will be met primarily through higher water bills and local fees, according to a study by the American Water Works Association (AWWA), PRWeb reported February 27. The report, titled "Buried No Longer: Confronting America's Water Infrastructure Challenge," analyzes many factors, including timing of water main installation and life expectancy, materials used, replacement costs, and shifting demographics. Nationally, infrastructure needs are almost evenly divided between replacement and expansion requirements. Cities will be impacted in different ways depending on size and geography. Many small communities will face the greatest challenges because they have smaller populations across whom to spread expenses. Source: http://www.prweb.com/releases/prweb2012/2/prweb9222932.htm

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168